

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering calendar year 2018

Date filed: February 22, 2019

Name of companies covered by this certification:

TelephoneYacht, LLC

832695

Name of signatory: Ather Mahmood

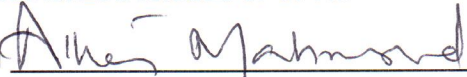
Title of signatory: CEO

I, Ather Mahmood, certify that I am an officer of the company named above, and acting as an agent of the companies, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement, consisting of the CPNI Compliance Policies and Operating Procedures of TelephoneYacht, LLC that describes the steps taken to protect CPNI and explains how the companies' procedures ensure that they are in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The companies have not taken any actions against data brokers in the past year.

The companies have not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed 
Ather Mahmood
CEO
TelephoneYacht, LLC

Attachments: Accompanying statement explaining CPNI procedures.

CPNI Compliance Policies and Operating Procedures of TelephoneYacht, LLC.

TelephoneYacht, LLC (herein referred to as “TelephoneYacht” or “Company”) has the following policies and procedures to protect the confidentiality of Customer Proprietary Network Information (“CPNI”) pursuant to the Federal Communications Commission (“FCC”) rules set forth in 47 C.F.R. Part 64, Subpart U, sections 2001 *et seq* implementing section 222(c) of the Communications Act of 1934, as amended.

CPNI is defined as “(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.” 47 U.S.C. § 222(h)(1).

The Company has developed policies and operating procedures designed to protect such CPNI from data brokers, pretexters, or any other type of unauthorized access, as outlined below in detail.

I. Use, Disclosure, and Access to CPNI

In accordance with 47 U.S.C. § 222(c) and 47 C.F.R. §§ 64.2001 *et seq*, TelephoneYacht has implemented policies and operating procedures to allow disclosures of CPNI only where permitted.

A. Use of CPNI without Customer Approval

TelephoneYacht may use, disclose, or permit access to CPNI, without customer approval, for: billing and collection; administrative customer care services; maintenance and repair services; to protect its rights or property; to protect its customers and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, its services; responding to a lawful law enforcement request for such information; or use of aggregate customer information. With respect to third party vendors, including those providing inside wiring installation, maintenance, and repair services on the Company’s behalf, such vendors are subject to nondisclosure agreements with respect to any CPNI they may obtain. The Company does not use CPNI for marketing purposes at this time.

B. Use of CPNI with Customer Approval

TelephoneYacht does not currently use CPNI in a manner that requires prior customer approval. Should the Company change this policy, it would seek approval from and give notice of rights to its Customers pursuant to 47 C.F.R. §§ 64.2007–64.2008 for any use, disclosure or access to CPNI requiring customer approval. As required, the Company’s CPNI Compliance Officer would maintain records of all notifications and requests for approvals.

II. Safeguards against Unauthorized Use or Disclosure of or Access to CPNI to Unauthorized Parties

In accordance with 47 U.S.C. § 222(c) and 47 C.F.R. §§ 64.2001 *et seq*, TelephoneYacht has policies and operating procedures to safeguard against any unauthorized use or disclosure of CPNI to unauthorized parties.

A. Safeguards on Use, Disclosure of or Access to CPNI

Pursuant to 47 C.F.R. § 64.2009, TelephoneYacht has implemented a system to safeguard against any unauthorized use, disclosure of or access to CPNI. The Company does not currently use, disclose, or permit access to CPNI for marketing. Any contemplated use, disclosure of or access to CPNI for marketing purposes will require senior management review and, if approved, the Company will implement any necessary safeguards as required under the FCC's rules.

1. Training

As required by 47 C.F.R. § 64.2009(b), TelephoneYacht trains all employees regarding the CPNI policies and operating procedures. The training program outlines when the employees are or are not authorized to use, disclose or permit access to CPNI and the disciplinary process if CPNI policies and/or operating procedures are violated, up to and including termination of employment.

The Company trains its employees to identify a "breach" as defined in the FCC's rules. Employees are instructed to contact the CPNI Compliance Officer immediately if they become aware of, suspect or attempt any breaches of CPNI. The CPNI Compliance Officer will determine if a breach has occurred and take appropriate steps pursuant to 47 C.F.R. § 64.2011 and the Company's internal policy and operating procedures on reporting CPNI breaches to law enforcement.

It is the Company's policy that all employees report any suspected breach regardless of external or internal origin, including the employee's own actions. Employees that fail to report an intentional or unintentional breach caused by their own actions will be disciplined more severely than employees who come forward immediately.

2. CPNI Compliance Officer

As required by 47 C.F.R. § 64.2009(e), TelephoneYacht appointed Rabia Mahmood as its CPNI Compliance Officer. The CPNI Compliance Officer is responsible for filing the Company's annual CPNI compliance certifications, maintaining records regarding CPNI, and monitoring and enforcing its policies and operating procedures internally.

The CPNI Compliance Officer is responsible for making any reports to the FCC if opt-out mechanisms do not work properly pursuant to 47 C.F.R. § 64.2009(f) or any reports of breach of CPNI to the United States Secret Service and Federal Bureau of Investigation pursuant to 47 C.F.R. § 64.2011.

The CPNI Compliance Officer maintains for at least two (2) years a record of any disclosures, notices to customers regarding rights, suspected breaches, reported breaches, and any and all other information related to CPNI and the enforcement of these policies and operating procedures. The CPNI Compliance Officer will also revise and update these policies and operating procedures as needed to address any concerns that arise in their application.

B. Safeguards on Disclosure of CPNI

In order to discover and protect against attempts to gain unauthorized access to CPNI and pursuant to 47 C.F.R. § 64.2010, TelephoneYacht has implemented a system to detect and protect against any unauthorized disclosure of CPNI.

In addition to the Company's policies and operating procedure, all electronic formats of CPNI are protected using best security practices. The Company's servers are stored in a locked room within the Company's office. Additionally, the Company limits internal access to CPNI to select employees based upon specific need to access CPNI. These select employees may only access CPNI after providing their proper login and password, which must be changed periodically for greater protection.

The Company physically secures CPNI in a room with an electronic lock or within locking filing cabinets. During normal business hours, a Company employee is stationed inside the front entrance and only unsecured entrance into the office. Outside of normal business hours, the Company's office is secured by an electronic lock and an alarm system.

1. Telephone Access to CPNI

As required by 47 C.F.R. § 64.2010(b), TelephoneYacht authenticates its Customers without the use of readily available biographical information or account information when a Customer initiates telephone contact. A proper password pursuant to 47 C.F.R. 64.2010(e) is required before anyone discloses any CPNI to a Customer via telephone.

If a Customer cannot be authenticated or provide the correct password, the Company calls the Customer at the telephone number of record or provides the information by mail via the address of record.

2. Online Access to CPNI

In accordance with 47 C.F.R § 64.2010(c), TelephoneYacht allows its Customers to access CPNI online through a system that requires authentication and a password. If any account information, including password, backup authentication method, online account or address of record is changed, the Company notifies its Customers that there has been a change without revealing the changed information pursuant to 47 C.F.R 64.2010(f).

All of the Company's Customers are business customers, and the business customer exemption set forth in 47 C.F.R. § 64.2010(g) should apply.

The Company does not have any retail stores, so the requirements set forth in 47 C.F.R. § 64.2010(d) are not applicable.

III. Reporting CPNI Breaches to Law Enforcement

In accordance with 47 C.F.R. § 64.2011, TelephoneYacht has implemented policies and operating procedures governing reporting CPNI breaches to law enforcement. Any employee that becomes aware of, suspects or attempts any breaches of CPNI must report such information to the Company's CPNI Compliance Officer immediately. No reports or disclosures will be made to the customer except as allowed under 47 C.F.R. § 64.2011(b)-(c).

Upon learning of a breach, the Company will notify the United Secret Services and Federal Bureau of Investigation using the link: <http://www.fcc.gov/eb/cpni>. In no event will this notification be later than seven (7) business days after a reasonable determination of the breach. If the Company believes there

is an extraordinary urgent need to notify its Customer, it shall indicate this in its notification. The Company shall cooperate with the investigating agency, including not notifying the customer if instructed by the investigating agency.

If the Company does not receive instruction from law enforcement after seven (7) business days of its report, it will notify its Customer of the breach. The Company follows state law customer notification requirements to the extent state law is not inconsistent with 47 C.F.R. § 64.2011.

The Company's CPNI Compliance Officer is responsible to maintain a record for two (2) years of any breaches and subsequent notifications made to law enforcement. These records shall include the "dates of discovery and notification, a detailed description of the CPNI that was subject of the breach, and the circumstances of the breach." 47 C.F.R. § 64.2011(d).